## LISTING OF CLAIMS:

1. (Currently Amended) A method in a data processing system for managing access to data in a keystore, the method comprising:

receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase;

responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using [[the]] a second key to form a decrypted item of data; and

sending the decrypted item of data to the requestor.

2. (Original) The method of claim 1, wherein the requestor is an application.

3. (Canceled)

4. (Original) The method of claim 1, wherein the item of data is another key.

5. (Original) The method of claim 1, wherein the item of data is a certificate.

6. (Original) The method of claim 1, wherein the item of data is indexed within the Keystore using an alias.

7. (Original) The method claim 6, wherein the request includes the alias further comprising:

responsive to an absence of a determination that the requestor is a trusted requestor, returning a null result to the requestor.

8. (Original) The method of claim 1 further comprising:

responsive to receiving a request to add a new item of data to the Keystore, encrypting the new item of data to form an encrypted item of data; and storing the encrypted item of data in the Keystore.

9. (Currently Amended) The method of claim 8 further comprising:

storing an encrypted copy of the new item of data in the Keystore.

10. (Original) The method of claim 8, wherein each item of data in the Keystore is associated with an alias.

11. (Currently Amended) A method in a data processing system for managing access to data in a keystore, the method comprising:

receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase; and

responsive to a determination that the requestor is a trusted requestor, sending [[the]] a second key and an encrypted copy of the item of data to the requestor.

12. (Currently Amended) A Keystore system comprising:

a Keystore object including:

a key; and

a plurality of entries, wherein each entry within the plurality of entries is encrypted using the key; and

a Keystore process, wherein the Keystore process provides access to the plurality of entries in response to a request from a trusted application by providing the key to the trusted application and in response to a determination that the application is a trusted application, wherein the determination is performed by checking an application's identity against a trusted codebase.

13. (Original) The Keystore system of claim 12, wherein the plurality of entries is indexed using a plurality of aliases and wherein the request includes an alias for a requested entry.

14. (Currently Amended) The Keystore system of claim 12, wherein the plurality of entries is a first plurality of entries and wherein the Keystore object includes a second plurality of entries corresponding to the first plurality of entries ~~in an unencrypted form~~ encrypted with a second key.

15. (Currently Amended) A data processing system comprising:

a bus system;

a communications unit connected to the bus, wherein data is sent and received using the communications unit;

a memory connected to the bus system, wherein a set of instructions are located in the memory; and

a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to receive a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key, determine whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase, and send [[the]] a second key and an encrypted copy of the item of data to the requestor[[,]] in response to a determination that the requestor is a trusted requestor.

16. (Original) The data processing system of claim 15, wherein the bus system includes a primary bus and a secondary bus.

17. (Original) The data processing system of claim 15, wherein the processor unit includes a single processor.

18. (Original) The data processing system of claim 15, wherein the processor unit includes a plurality of processors.

19. (Original) The data processing system claim 15, wherein the communications unit is an Ethernet adapter.

20. (Currently Amended) A data processing system for managing access to data in a datastore, the data processing system comprising:

receiving means for receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

determining means for determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase; and

decrypting means, responsive to a determination that the requestor is a trusted requestor, for decrypting a copy of the item of data using [[the]] a second key to form a decrypted item of data; and

sending means for sending the decrypted item of data to the requestor.

21. (Original) The data processing system of claim 20, wherein the requestor is an application.

22. (Canceled)

23. (Original) The data processing system of claim 20, wherein the item of data is another key.

24. (Original) The data processing system of claim 20, wherein the item of data is a certificate.

25. (Original) The data processing system of claim 20, wherein the item of data is indexed within the Keystore using an alias.

26. (Original) The data processing system claim 25, wherein the request includes the alias further comprising:

returning means, responsive to an absence of a determination that the requestor is a trusted requestor, for returning a null result to the requestor.

27. (Original) The data processing systcm of claim 20 further comprising:

encrypting means, responsive to receiving a request to add a new item of data to the Keystore, for encrypting the new item of data to form an encrypted item of data; and

storing means for storing the encrypted item of data in the Keystore.

28. (Currently Amended) The data processing system of claim 27, wherein the storing means is a first storing means further comprising:

second storing means for storing an encrypted copy of the new item of data in the Keystore.

29. (Original) The data proccssing systcm of claim 27, wherein each item of data in the Keystore is associatcd with an alias.

30. (Currently Amended) A data processing system for managing access to data in a datastore, the data processing systcm comprising:

receiving means for receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

determining means for determining whether the requestor is a trusted requestor, wherein the dctermining step is performed by checking a requestor's identity against a trusted codebase; and

sending means, responsive to a determination that tbe requestor is a trusted requestor, for sending [[the]] a second key and an encrypted copy of the item of data to the rcquestor.

31. (Currently Amended) A computer program product in a computer readable medium for managing access to data in a datastore, the computer program product comprising:

first instructions for receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

second instructions for determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase; and

third instructions, responsive to a determination that the requestor is a trusted requestor, for sending [[the]] a second key and an encrypted copy of the item of data to the requestor.

32. (Currently Amended) A computer program product in a computer readable medium for managing access to data in a datastore, the computer program product comprising:

first instructions for receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

second instructions for determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase;

third instruction, responsive to a determination that the requestor is a trusted requestor, for decrypting a copy of the item of data using [[the]] a second key to form a decrypted item of data; and

fourth instructions for sending the decrypted item of data to the requestor.